Business Considerations and Foundations for Assuring Software Security: Business Case Models for Rational Action

Don O'Neill, Software Engineering Institute [vita[1]]

2008-10-24

L1 / L, M[2]

In this article, we discuss business considerations and business case models for assuring software security. Specifically, we review industry forces and enterprise considerations that feed into business case models.

Overview

Business case models describe what activities a firm could perform, how it will perform them, and when it will perform them [Afuah 03[3]]. A good business model should serve as a design [Fischer 06[4]]. The only proper purpose of that design should be to ensure the greatest possible competitive advantage for the business [Afuah 03[5]].

Toward that end, the business case model should help decision makers integrate a wide range of potential considerations—such as resources, product-market position, and profitability—into a solution that will ensure the best performance for their corporation [Afuah 03[6]]. With respect specifically to the security and trustworthiness of software, business case models should help decision makers understand, implement, verify, and oversee an effective enterprise-wide software assurance solution [Fischer 06[7]].

Common sense alone might dictate that the business case model for building security into the software process will have these two important dimensions: (1) business and (2) technical. But a good business case model for software assurance should unify those dimensions in the enterprise's technology infrastructure and strategic management.

This article examines how those two dimensions can work together to assure software product security and reliability. It is intended to provide general guidance for BSI readers who are just starting to think about this area. Some of these topics are discussed in more detail in other BSI Business Case[8] articles and in the BSI System Strategies[9] material.

Business Considerations

The business case model framework assists in reasoning about the software security decision process. It can be used to guide the selection of models appropriate for the enterprise and assist in their instantiation with local factors that best characterize the business environment and enterprise culture. Several considerations influence the organization's development of a business case for assuring security:

- Is security viewed as a cost or an investment?
- Are security solutions viewed as commoditized or strategic?
- Does the organization seek only protection or does it strive to achieve resilience?
- Is the security approach inward looking and limited to a single system or outward looking to a system of systems and its dependencies?

1. http://buildsecurityin.us-cert.gov/bsi/about_us/authors/681-BSI.html (O'Neill, Don)
3. #dsy676-BSI_afuah03
4. #dsy676-BSI_fischer06
5. #dsy676-BSI_afuah03
6. #dsy676-BSI_afuah03
7. #dsy676-BSI_fischer06
8. http://buildsecurityin.us-cert.gov/bsi/articles/knowledge/business.html (Business Case Models)
9. http://buildsecurityin.us-cert.gov/bsi/articles/best-practices/system-strategies.html (System Strategies)

The organization's perspective on these questions will determine the enablers and barriers to assuring software security. The chief security officer (CSO) is expected to lead the enterprise in making an explicit commitment to the goal of assuring software security and in determining the framework for achieving it (Figure 1[10]).

Figure 1: Business considerations overview

Understanding the Driving Forces of the Software Industry

The forces that we see at work in the software industry, and which we frequently read about, include the ability for organizations to compete on a global platform, not just nationally. The ability to develop and modify software quickly is essential for us to remain innovative and competitive. We see the following driving forces affecting the software industry.

Global Software Competitiveness

Global software competitiveness, a critical ingredient to the nation's prosperity, is centered on controlling scarce personnel resources, valued customers, competitors, and event threats. The Global Software Competitiveness Program sponsored by the Center for National Software Studies provides fundamental observations on global software competitiveness and an assessment tool [O'Neill 02a[13]].

10. #dsy676-BSI_figure1
13. #dsy676-BSI_oneill02a

With the emergence of Global Software Development [Carmel 99[14]] as a business model to produce software products rapidly, there is a need to obtain deep understanding of global software competitiveness and security and the leading indicators that permit systematic reasoning about it.

Software as the Carrier for Innovation

The nation is dependent on information systems technology. Software is the means by which innovation is expressed in nearly every industry sector [NSG 05[15]]—and fortunately so, because software can be readily changed in response to the rapid innovations in those sectors. It is in fact the changeable nature of software that enables industry sectors to compress time to market.

Software's operations range from rules-based transactions to process transformations. As a result of integrated telecommunications, data repositories, and high performance computing, previously unsolved problems are being tackled. Not only is software the linchpin of the technology sector, software is also central to innovation in most industry sectors.

Software Assurance Scope

Concerns about software assurance are also emerging as an industry force. Software assurance relates to "the level of confidence that software functions as intended and is free of vulnerabilities" [CNSS 06[16]].

The U.S. Department of Defense (DoD) suggests that the guiding principle of software assurance is to understand a systems perspective. For the DoD, the scope of software assurance is governed by "the level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software" [DoD 05[17]]. Here the focus is systems and their harmonious operation.

The Department of Homeland Security (DHS) is facilitating "a national public-private effort to promulgate best practices and methodologies that promote integrity, security, and reliability in software code development, including processes and procedures that diminish the possibilities of erroneous code, malicious code, or trap doors that could be introduced during development" [DHS 03[18]]. Here the focus is the software component and the methods of construction to build security in.

Understanding the Driving Forces of the Enterprise That Is Dependent on Software-Intensive Systems

Organizations that are dependent on software-intensive systems need to be concerned about the cost and benefits associated with such systems. We believe that most medium to large organizations have such a dependency. These organizations need to be concerned about the cost and benefit of investment in cyber security. Forces that should be considered include due diligence on behalf of customers, strategic (marketing) decision making, consideration of whether security assurance is viewed as a cost or an investment, and the tension between competitiveness and security.

Theory of Expected Utility

Simply put, the Theory of Expected Utility [Poulton 94[19]] favors outcomes that obtain the most benefit and incur the least loss. Under this theory, an enterprise with a goal whose achievement is not guaranteed by either the state of the art or the state of the practice may choose to select another goal. The goal to achieve software security is an example of this theory [CIO 06[20]].

14. #dsy676-BSI_carmel99
15. #dsy676-BSI_nsg05
16. #dsy676-BSI_cnss06
17. #dsy676-BSI_dod05
18. #dsy676-BSI_dhs03
19. #dsy676-BSI_poulton94
20. #dsy676-BSI_cio06

However, an enterprise has an obligation and a fiduciary responsibility to apply due diligence on behalf of its customers, its stockholders, and the public. Consequently, it has a need to establish an enterprise software security assurance operation. Instead of a goal to achieve software security, then, the enterprise establishes the goal to operate an effective software security assurance program.

Commoditized and Strategic Decision Making

The current approach to cyber security policy is market driven; consequently, the outcome is governed by industry decision-making dynamics. It is important to know that the pursuit of security is a cost and the achievement of security may yield a strategic advantage, although so far no one has managed to characterize that benefit in concrete terms.

It is also important to know that cost is a function of perceived value, an understanding that seems to be largely lacking in the general case of secure software. This lack is understandable: If an enterprise expends little or nothing on security while its competitors are incurring expense in the pursuit of the illusive goal of security, that free-riding enterprise will get some margin of competitive advantage because it will be able to sell its products cheaper at greater profit.

An enterprise may obtain a strategic advantage from the successful pursuit of security. Further, if customers demand verifiable security as a condition of purchase, the company that can ensure it will have a distinct competitive advantage. However, the only way it can realize an advantage is if customers value security highly enough to pay the additional cost of providing it. If price is the only criterion, though, the additional cost of ensuring secure functioning will probably reduce competitiveness by driving up the price.

Cost and Investment

When commoditized security solutions with their emphasis on compliance are chosen, security expense is viewed as a cost. When strategic security solutions are sought to improve competitiveness, security expense is viewed as investment.

CIOs are invited to explore their competitiveness versus security tradeoffs [O'Neill 02b[21]] by visiting the assessment tool at http://members.aol.com/ONeillDon2/comp-sec_frames.html [O'Neill 02c[23]].

Constructing the Enterprise Assurance Infrastructure for Software Trustworthiness and Security

One way to establish organizational assurance infrastructure is to name a chief security officer (CSO) and to define a security framework that the CSO operates in. Once this framework exists, the organization is in a better position to reason about security return on investment, business continuity, and the implications for systems or systems of systems.

CSO Security Framework

The CSO needs a security framework that packages the capabilities to achieve cyberspace security readiness into defined products and services that secure the project suite. The vision for a security framework needs to meet several objectives, including understanding the costs, avoiding lawsuits, protecting the business, protecting the critical infrastructure, and controlling the disclosure of information. This vision can be realized by systematically

- promoting awareness and obtaining commitment
- conducting basic training in security practices
- performing due diligence
- ensuring the continuous operation of systems critical to the enterprise

21. #dsy676-BSI_oneill02b
23. #dsy676-BSI_oneill02c

- controlling the dissemination of information

Security Return on Investment

With the dramatic increase in cyberspace incidents and perceptions about the high cost of investment for security readiness and survivability, there is a need for a method to reason about and compute security return on investment (ROI) [O'Neill 07[24]].

A common industry security ROI methodology would deliver numerous benefits. The contributors to security readiness, the costs to achieve security readiness, and the costs to recover from cyberspace incidents would be better understood. The enterprise could reason about its security investment decision with increased precision. In practical terms security ROI is the value of loss prevention less its cost. For instance, if a grocery store installs a security system to prevent the theft of its inventory, then the return on that investment is the dollar difference between losses prior to the system's installation and after it was installed. The investment itself is the cost of the loss prevention system. In that respect, the cost of the security system can be justified if the loss prevention savings is greater than the cost of the system.

We calculate ROI by evaluating the expression [ROI: = Savings/Cost], where savings is cost avoidance resulting from resistance, recognition, and reconstitution efforts and cost includes preparation and incident cost. Incident cost is cleanup, lost opportunity, and critical infrastructure impact. Other methods for calculating ROI can be found in the literature.

CIOs and CSOs are invited to explore their security return on investment by visiting the companion Calculating Security Return on Investment[25] article or by visiting the assessment tool[26] [O'Neill 06b[27]].

Business Continuity: Protection and Resilience

In the past, the security effort has been concentrated on avoiding threats and vulnerabilities. In the future, the focus must shift to sustaining business continuity. Critical systems of systems must be resilient even under stress, and owners need to be able to agree on and exert operational control under all circumstances of use. The means to do this include coordinated recovery time objectives, established interoperability standards, distributed supervisory control protocols, and distributed and replicated data architectures [O'Neill 08a[28]]. Further development is needed in these areas.

Systems and Systems of Systems

The challenge in constructing a business case is to characterize the appropriate knowledge, skills, behaviors, and practices that enable the preferred security approaches for the type of product element being secured. This assessment becomes the core of the infrastructure implementation challenge of the CSO and the basis for transforming and assuring software security operations. Systems of systems have many users but are lacking when it comes to clear ownership.

Implementing the Enterprise Assurance Infrastructure for Software Trustworthiness and Security

The infrastructure needed to support software security assurance and its oversight is multidimensional. Within each dimension there are potential barriers that may impede the transition to improved security and potential enablers that may advance the transition. Some of these factors include public policy, technology, education, sourcing, standards and best practices, and measurement.

24. #dsy676-BSI_oneill07
25. http://buildsecurityin.us-cert.gov/bsi/articles/knowledge/business/677-BSI.html (Calculating Security Return on Investment)
26. http://members.aol.com/ONeillDon2/sec-roi_frames.html
27. #dsy676-BSI_oneill06b
28. #dsy676-BSI_oneill08a

When implementing assurance infrastructure, some special considerations include the impact of outsourcing, steps needed to assure open source software, the use of knowledge networks to facilitate coordination and collaboration, and methods for managing an assurance crisis.

Assuring Software Security when Outsourcing Software Development

Studies on global software competitiveness conducted by the Center for National Software Studies reveal that offshore outsourcing of software development is a tactic that delivers a competitive advantage. As global enterprises increasingly seek to achieve competitiveness on the cheap, global outsourcing is becoming more widespread. But due diligence is needed if success in outsourced software development is to be achieved [O'Neill 08b[29]]. What should global enterprises look for in an outsourcing partner?

An innovation [USPTO 04[30]] capable of managing to scale the initiation of global enterprise projects and their fulfillment by offshore vendors also provides a framework to assure software security. Driven by skills, cost, commoditization, innovation, risk, and scale considerations, the innovation disassembles the supply chain of the software project life cycle and repackages the defined processes, practices, and capabilities (including their underlying knowledge, skills, and behaviors) into a pipeline of managed and controlled onshore and offshore nodes of repeatable services. Those nodes can be arranged as needed to strike the right balance and fit among the drivers.

Assuring Open Source Software

Open source is a commodity product by definition. Open source is ordinarily accompanied by a license that requires users to maintain the program as open source. Interestingly, major suppliers like IBM and Microsoft are moving away from the proprietary model for certain product categories [Samuelson 06[31]]. These suppliers, however, retain a stake in the open source repository. For example, IBM dedicates 600 programmers to sustaining the Linux open source. In part, the open source movement is market driven; in part, suppliers are conceding commoditization for a portion of the product stack. Open source evolution is driven by users who submit changes. These changes are not simply change requests in the form of requirements or hoped for capabilities; instead they are the actual source code implementation of the change a user hopes to see adopted by the community. In the past four years, for the Linux open source product, there have been 38,000 changes delivered by 1,000 contributors; 20 contributors have authored 50% of those changes [O'Neill 06b[32]].

Despite drivers on both sides, the choice of open source or closed source is considered to be security neutral. Open source is available to potential hackers, but it is also under continuous peer review and inspection by a diverse audience. Open source quality is assisted by many practitioners inspecting source code components and rapid correction and dissemination of corrections. While support is generally available within the community of users, however, there is a lack of accountability. The Total Cost of Ownership is situational. While the open source product is free and licensed, a user must incur hardware, other software, training, conversion, and other support costs. In addition, due diligence requires a user to field a staff knowledgeable in the open source code base used. Underscoring the cost attractiveness of open source, there is a zero marginal cost of scale because open source doesn't require additional licenses as an installation grows.

Knowledge Networks

Knowledge networks are needed to facilitate communities of practice. The knowledge networks associated with the Government Orbit and the Commercial Orbit represent two distinct audiences with different perspectives. Consequently, interest-driven, small-world networks organized around the different perspectives need to be formed for each of these orbits to facilitate collaboration and coordination. Forming these knowledge networks is expected to improve accuracy, speed, tolerance, and scalability in knowledge

29. #dsy676-BSI_oneill08b
30. #dsy676-BSI_uspto04
31. #dsy676-BSI_samuelson06
32. #dsy676-BSI_oneill06b

sharing outcomes and to promote the social interaction capable of producing innovative solutions needed for problem solving and crisis management.

Crisis Management

A crisis is an unstable situation. Crisis management comprises the systematic steps of prevention and response that sustain stability or result in a return to stability. Crisis management starts with crisis prevention, which includes identifying a crisis, planning a response to the crisis, and confronting the crisis. Crisis management concludes with crisis response and resolution, which ideally involves executing a plan for an identified crisis. Preliminary measures need to be taken to prevent a crisis. The enterprise should plan ahead, project likely outcomes, and avoid decisions that have the potential to trigger a crisis.

While crisis management builds on risk management, its focus is different in one important respect. Using risk management, a potential risk might be identified and the risk resolution might be to do nothing based on a low probability, high cost argument. In choosing avoidance over sustainment, an organization might find itself depending on risk management to consider the probability of one event or another. As a result, the organization would evaluate the propagation effects of those events but would not plan and provide for the recovery and switchover capabilities needed to ensure continuous operation. Managing risk to avoid a risk event produces outcomes that are different from planning to withstand the occurrence of the risk event and execute follow-up steps. Crisis management uses the risk management process but then presses ahead to the stages of response and resolution.

Verifying and Overseeing the Enterprise Assurance of Software Trustworthiness and Security

Verification and oversight of assurance are key process elements once an enterprise software assurance program has been established. Assessing business case factors initially and on an ongoing basis also contributes to improving the organization’s software assurance position.

Verification and Oversight

Verifying the enterprise assurance of software trustworthiness and security is achieved through demonstration and assessment, including industry state of the art and state of the practice, enterprise assessment of assurance infrastructure, enterprise assessment of technical foundations, and demonstration of enterprise survivability and resilience.

Overseeing the enterprise assurance of software trustworthiness and security is achieved through executive and senior management oversight and board of directors’ oversight, focusing on appropriate aspects of enterprise operations, process, culture, training, and actual demonstration.

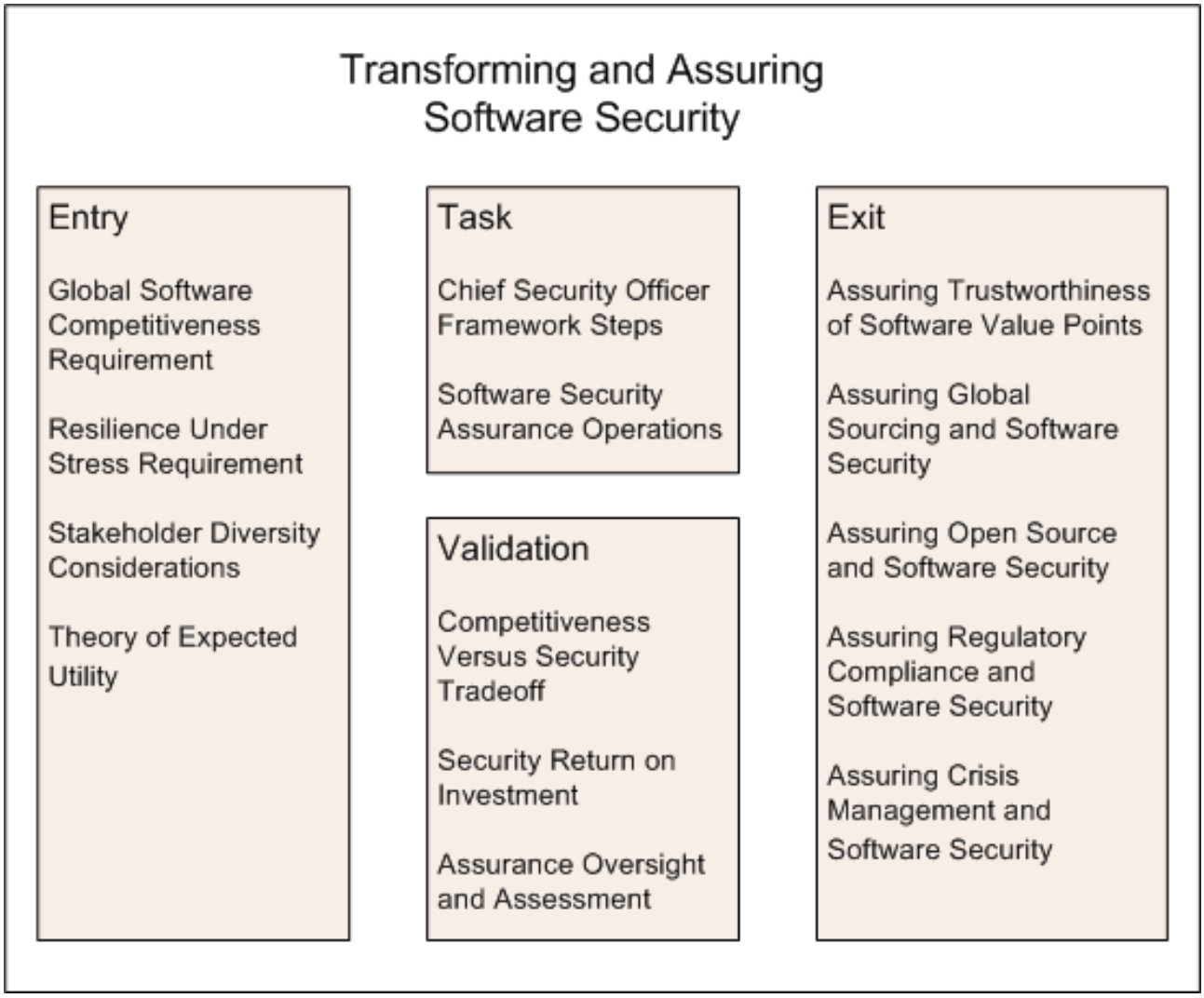
Assessing Business Case Factors

The following questions are useful in promoting focus on the business case factors associated with assuring software security:

- To what extent are software security assurance foundations considered to be in place within the industry?
- To what extent is the organization’s competitiveness traded off for security?
- Does the organization treat security expense as a cost or investment?
- Has management made an explicit commitment to a security goal?
- Has management made an explicit commitment to a method for achieving the security goal?
- Does the organization seek to achieve protection or resilience?
- To what extent does the organization use a thin client architecture?
- To what extent does the organization use a single vendor’s products?
- To what extent is the organization compliance-driven or business-value driven?

- To what extent are recovery time objectives coordinated among the dependent systems of the organization?
- Does the organization compute a security ROI?
- Does the ROI calculation include terms for cleanup, lost opportunity, and reconstitution?
- To what extent does the organization use a defined software security infrastructure operation?
- To what extent are the organization enablers to assuring software security understood and being utilized? List the enablers.
- To what extent are the organization barriers to assuring software security understood and being dealt with? List the barriers.
- To what extent does the organization include its global supply chain management operation in its software security assurance operations?
- To what extent are the management staff and technical staff trained in their software assurance management responsibilities?
- To what extent is the organization legal staff trained in software security assurance?
- To what extent are organization executive and senior management trained in their software assurance management responsibilities?
- To what extent are the members of the board of directors informed of their software security assurance oversight responsibilities?

Figure 2: Transforming and assuring software security



References

[Afuah 03]	Afuah, Allan. *Business Models: A Strategic Management Approach*. New York, NY: McGraw-Hill, 2003.
[Carmel 99]	Carmel, Erran. *Global Software Teams*. Englewood Cliffs, N.J: Prentice Hall, 1999.
[CIO 06]	Holmes, Allan. "The Global State of Information Security[34]." *CIO*, September 15, 2006, pp. 82-94.
[CNSS 06]	The Committee on National Security Systems. *National Information Assurance (Ia) Glossary CNSS Instruction No. 4009 Revised June 2006*[35].
[DHS 03]	Department of Homeland Security. *National Strategy to Secure Cyberspace*[36]. Action-Recommendation 2-14, February 2003.
[DOD 05]	Department of Defense. *DoD Software Assurance Initiative*[37], September 13, 2005.
[Fischer 06]	Fischer, Henning. *Business Case Modeling for Design*[38]. Adaptive Path, LLC, August 28, 2006.
[NSG 05]	National Software Strategy Steering Group. "Software 2015: A National Software Strategy to Ensure U.S. Security and Competitiveness[39]." Center for National Software Studies, April 29, 2005.
[O'Neill 02a]	O'Neill, Don. "Global Software Competitiveness Assessment Tool[40]." (2002).
[O'Neill 02b]	O'Neill, Don. "Competitiveness Versus Security[41]." Keynote Presentation, Quality Week 2002 Conference, San Francisco, CA, September 2002.
[O'Neill 02c]	O'Neill, Don. "Competitiveness Versus Security Tradeoff[42]."
[O'Neill 06a]	O'Neill, Don. "Security Return on Investment Interactive Worksheeet[43]." (2006).
[O'Neill 06b]	O'Neill, Don. "Criteria and Guidance for Peer Review of Open Source Artifacts[44]." *The Competitor 10*, 1 (September 2006).
[O'Neill 07]	O'Neill, Don. "Calculating Security Return on Investment[45]." *Build Security In* web site, February 2007.
[O'Neill 08a]	O'Neill, Don, "Maturity Framework for Assuring Resiliency Under Stress[46]." *Build Security In* web site, July 2008.
[O'Neill 08b]	O'Neill, Don, "Inside Track to Offshore Outsourcing Using the Trusted Pipe", Making the Business Case for Software Assurance Workshop, Carnegie Mellon University, Pittsburgh, PA, 26 September 2008.

[Poulton 94]	Poulton, E. C. *Behavioral Decision Theory: A New Approach*. Cambridge, England: Cambridge University Press, 1994 (ISBN 0521443687).
[Samuelson 06]	Samuelson, Pamela. “Regulating Technical Design.” *Communications of the ACM 49*, 2 (February 2006): 25-30.
[USPTO 04]	United States Patent Application Published for Review, Publication Number US 2006-0015384, Application Number 10/890,221. “Business Management and Procedures Involving Intelligent Middleman.” Filing Date 7/14/2006.

Carnegie Mellon Copyright

1. mailto:permission@sei.cmu.edu